

The Fix • Analysis

What we know about the 21 states targeted by Russian hackers

By **Callum Borchers** September 23, 2017

This post has been updated.

The Department of Homeland Security was short on details when it [said](#) Friday that it had notified 21 states of Russian efforts to hack their election systems in 2016. For one thing, the department didn't publicly identify the states. For another, it didn't say how many of the hacking attempts were successful — or to what degree.

Based on reporting by The Washington Post, Associated Press and other news outlets — plus statements issued by some state officials — we now have a complete list of the affected states. The Fix has mapped and categorized them, according to what we know about the success or failure of the cyberattacks.

One trend that emerges in officials' remarks is a desire to strike a balance between projecting confidence in the integrity of vote tallies and concern about future threats.

For example: Wisconsin Secretary of State Doug La Follette (D) told me on Saturday that although a cyberattack on his state was unsuccessful, hacking is “for sure” a greater concern than voter fraud, which President Trump has [called](#) a “big problem.”

“We need Congress and the president to help states with their security systems for elections and ensure funding for more secure equipment where needed, and we need it to happen now,” Connecticut Secretary of State Denise Merrill (D) said. “Rather than investigating this attack on our democracy from a hostile foreign power, the Trump administration has formed a commission to prove that he won the popular vote, an idea that has been entirely discredited by numerous studies.

“Meanwhile, the cyber threat to our election systems remains and state election officials needed to know what was really going on so that we could respond and put in place any possible additional security measures.”

Oregon Secretary of State Dennis Richardson said “between hacking and voter fraud, in Oregon, I am most concerned about the sophistication of today's hacking attempts. We are doing everything we know how to do to ensure the safety of Oregon

Richardson declined to comment on Trump's priorities, as did other Republican officials contacted by The Fix.

Breached

Illinois

There is no evidence that votes were altered but, as previously reported, personal information for tens of thousands of voters was exposed. Here's a neat summary of what happened, [from Bloomberg](#):

In early July 2016, a contractor who works two or three days a week at the state board of elections detected unauthorized data leaving the network, according to Ken Menzel, general counsel for the Illinois board of elections. The hackers had gained access to the state's voter database, which contained information such as names, dates of birth, genders, driver's licenses and partial Social Security numbers on 15 million people, half of whom were active voters. As many as 90,000 records were ultimately compromised.

Time magazine [reported](#) in June that “congressional investigators are probing whether any of this stolen private information made its way to the Trump campaign.”

Sorta breached

Arizona

The Post's Sari Horwitz, Ellen Nakashima and Matea Gold [report](#) that “in Arizona, the Russian hackers did not compromise the state voter registration system or even any county system. They did, however, steal the username and password of a single election official in Gila County, state officials said.”

Targeted but not breached

Alabama

In a statement, the Alabama secretary of state's office said Homeland Security notified it of “suspicious traffic from IP addresses connected to election-related activity” but reported that “Alabama's system protections and preparations were successful in thwarting attempted hackers from breaching state networks and voting systems during the attacks.”

“While it is encouraging that our efforts to protect Alabamians' data have proven to be successful, we must remain vigilant and prepared for the constantly evolving threats to our voting systems and the integrity of those processes,” said Secretary of State John H. Merrill. “We will utilize every resource available to ensure we are protecting the data of all Alabamians.”

Alaska

“We were informed ... that we were one of 21 states that possibly were the target of an unsuccessful Russian-affiliated cyber incident in October 2016,” Elections Director Josie Bahnke said in a statement.

Bahnke's department emphasized that “Internet security protocols followed by the state of Alaska successfully protected our system, and the attempted probe had no effect on Alaska's voter registration and election management database or outcome of the election.”

California

Secretary of State Alex Padilla said in a statement that he has “no information or evidence that our systems have been breached in any way.” He also vented his frustration that Homeland Security did not tell him about the cyberattack sooner.

“It is completely unacceptable that it has taken DHS over a year to inform our office of Russian scanning of our systems, despite our repeated requests for information,” Padilla said. “The practice of withholding critical information from elections officials is a detriment to the security of our elections and our democracy.”

Colorado

Secretary of State Wayne W. Williams downplayed the hacking threat. “This was a scan, and many computer systems are regularly scanned,” he said in a statement. “It happens hundreds, if not thousands, of times per day. That's why we continue to be vigilant and monitor our systems around the clock.”

Connecticut

Secretary of State Denise Merrill put a positive spin on the hack attempt in an [interview](#) with the Hartford Courant. “In essence, this is good news for us because our system worked and turned back whatever targeting was done,” she said. “It does tell me that we need to be vigilant on this.”

Delaware

Election Commissioner Elaine Manlove seemed surprised that her state was targeted. “To be honest, I never thought Delaware would be one because it's so small,” she [told](#) the News Journal of Wilmington.

“I've been in elections a long time, and we've never had problems,” she added. “We pride ourselves on our security, but you wonder, does somebody else up the game?”

Florida

“This attempt was not in any way successful, and Florida's online elections databases and voting systems remained secure,”

the Florida Department of State said in a statement.

Iowa

Secretary of State Paul Pate [told](#) the Des Moines Register that there were unsuccessful “attempted outside intrusions.”

Minnesota

Secretary of State Steve Simon said in a statement that “scanning from outside entities is commonplace and happens every day, which is why I continue to believe the most serious challenge to the integrity of our election system is the threat of outside forces, including foreign governments, who seek to disrupt and undermine our elections.”

North Dakota

Secretary of State Al Jaeger said his state’s “election systems were targeted, but not breached, in the summer of 2016. Security measures in place to protect these systems have proven to be effective, and we continue to update cybersecurity protections as new potential means of targeting are identified.”

Ohio

“DHS reported to us an incident,” Sam Rossi, a spokesman for Secretary of State Jon Husted, [told](#) Politico. “However, it lasted less than a second, and no security breach occurred. Nothing.”

Oklahoma

Bryan Dean, a spokesman for the Oklahoma State Election Board, [told](#) the Tulsa World that “before this, we were not aware of any attempts to get into our systems at all. This really didn’t get that far. No penetration was made into any system, and no further activity occurred.”

Oregon

Oregon's chief information security officer, Lisa Vasa, said in a statement that her team blocks “upwards of 14 million attempts to access our network every day. These attempts come from all over the world, including Russia, with the largest number from the U.S.”

Secretary of State Dennis Richardson called the unsuccessful breach attempt “a testament to the strength of the network security program we have in place.”

Pennsylvania

What we know about the 21 states targeted by Russian hackers ... <https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/...>
A spokesman for Gov. Tom Wolf (D) [told](#) the Associated Press that there is no evidence of a successful breach of state's election systems.

Texas

Sam Taylor, a spokesman for the secretary of state's office, [told](#) the Star-Telegram of Fort Worth that “to date, we have received no information indicating any elections-related systems in Texas have been compromised by bad cyber actors.”

Virginia

Commissioner of Elections Edgardo Cortés told The Post that would-be hackers scanned for vulnerabilities but failed to mount a successful attack.

Washington

Secretary of State Kim Wyman said in a statement that “the security protocols we already have in place made us aware of these attempted intrusions by Russian IP addresses throughout the course of the 2016 election. There was no successful intrusion, and we immediately alerted the Federal Bureau of Investigation of the activities.”

Wisconsin

“What this boils down to is that someone tried the door knob, and it was locked,” Reid Magney, a spokesman for the Wisconsin Elections Commission, told The Post.

Unclear

Maryland

State officials have not commented on the success or failure of any cyber attack.

 **367 Comments**

Callum Borchers covers the intersection of politics and media. He joined The Washington Post in 2015 from the Boston Globe, where his beats included national politics, technology and the business of sports. He is a former editor of Citizen's News in Naugatuck, Conn.

 Follow @callumborchers